网络空间安全面临的挑战与对策

冯登国　连一峰*
中国科学院软件研究所 北京 100190

摘要　当前全球网络空间安全形势持续演变，外部环境日趋严峻，网络安全问题时刻影响着政治、经济、军事、文化、科技等各个领域。为了有效防范重大网络威胁，掌握网络空间自主权和话语权，我们需要清醒认识网络空间面临的安全挑战，落实关键信息基础设施安全保护要求，重点加强数据安全和供应链安全保障能力，建立健全国家网络空间安全保障体系。

关键词　网络空间安全，关键信息基础设施，数据安全，供应链安全

DOI　10.16418/j.issn.1000-3045.20210813004

信息技术已经成为驱动和保障国家经济建设与社会发展的强力引擎，在能源、交通、金融、电信、制造、教育、文化等各个领域发挥着重要作用。国际社会间的合作、竞争和博弈也逐步拓展到网络空间，网络空间逐渐发展成为与陆、海、空、天并列的第五维空间领域，对国家安全产生了深远影响。

美国等西方发达国家频繁炒作“中国网络威胁论”，但实际上作为拥有最强大网络武器库、最先进网络基础设施的国家，美国一直依靠其强大的网络攻击能力，对包括中国在内的多个国家持续进行网络攻击；部分西方发达国家利用网络空间的信息不对称和技术门槛，推动网络霸权和数据霸权，进一步加剧信息壁垒和数字鸿沟，从而攫取政治利益和经济利益。与此同时，境内外敌对势力、高级持续性威胁（APT）组织、黑客组织每时每刻都在尝试对我国的关键信息基础设施、大数据平台和重要信息系统进行数据窃取、入侵渗透和攻击破坏；利用互联网络实施的隐私窃取、网络诈骗、敲诈勒索、恶意植入等网络违法犯罪活动也十分猖獗。这些破坏活动既阻碍了网络空间的发展，也给经济运行、社会发展和国家安全带来了严重威胁。

我国高度重视网络空间安全问题。2017 年 6 月 1 日，《中华人民共和国网络安全法》正式实施。这是我国第一部全面规范网络空间安全管理方面问题的基础性法律。2021 年 6 月 10 日，全国人民代表大会常务委员会审议通过《中华人民共和国数据安全法》，

*通信作者
资助项目：国家重点研发计划（2020YFB806504）
修改稿收到日期：2021年9月22日

自2021年9月1日起施行，目的是规范数据处理活动，保障数据安全，促进数据开发利用，保护个人、组织的合法权益，维护国家主权、安全和发展利益。国家网络安全职能部门依据法律和规章制度，采取了一系列维护网络空间安全的重大举措，包括保护关键信息基础设施、加强网络文化建设、打击网络恐怖和违法犯罪、完善网络治理体系、提升网络空间防护能力、加强网络空间国际合作等①。通过制订发布标准规范、开展专项整治行动、组织网络攻防实战演练、实施专项检查和督导等，有效提升了各行业单位和社会公众的安全意识，锻炼了针对重大网络安全事件的监测发现和应急处置能力，增强了安全保护弹性和攻防对抗能力，培养了一批训练有素的网络安全专业人才，初步建立了针对关键信息基础设施和重要信息系统的安全保障体系。

当前，国际国内形势纷繁复杂，全球网络空间安全态势持续演变，外部环境日趋严峻，我国在经济转型和社会发展方面也面临困难和压力，需要我们清醒地认识到网络空间所面临的安全挑战，并制定有针对性的应对策略。

1 挑战

1.1 针对网络空间主导权的争夺日益激烈

传统意义上网络威胁的内涵是指通过技术手段，利用目标对象的漏洞、缺陷或薄弱点，采取探测、渗透、入侵、提权、窃取、篡改等方式，破坏目标对象的机密性、完整性、可用性等安全属性。例如，入侵数据库以非法获取个人数据和敏感信息，向用户终端植入木马病毒以达到远程控制目的，或是发动大规模拒绝服务攻击造成网络应用服务中断。

当前，网络空间面临的威胁已不仅仅是上述针对网络与信息系统自身的攻击破坏。由于网络空间在社会层面的基础性支撑作用，利用网络空间掌握政治、经济、军事、文化、社会舆论等方面的话语权，从而为组织间乃至国家间的竞争对抗提供服务，已经成为国际社会的普遍做法。传统的针对网络和信息系统的破坏活动已经发展为通过控制网络空间，使其成为开展对抗竞争、获取政治或经济利益的重要工具和手段。近年来，国际社会频发的种族冲突、地域纷争和意识形态对抗，多次验证了网络空间已经成为掌握国际社会主导权，展现国家综合实力的重要体现。

例如，长期以来，美国凭借其在技术创新、产业引领与规则制定等方面的优势，持续掌控网络空间主导权。随着国际力量格局变化，网络空间的争夺加剧，给美国网络空间主导权带来前所未有的挑战。美国政府从调整理念、强化实力优势和谋求制度性权力3个维度着手，不断探索巩固与强化网络空间主导权的新举措。近年来，美国政府针对我国高科技领域陆续出台的一系列限制、打压政策，目的也是为了保持美国长期以来在信息技术领域的优势，把控全球网络空间的话语权，其相关动向对网络空间未来发展与力量格局均将带来深远影响[1]。

因此，我们必须要掌握网络空间发展的主动权，突破和掌握网络核心技术，坚持自主创新和开放融合②，全力保障网络安全。

1.2 跨领域、跨空间的渗透攻击频发

由于网络空间与物理空间、社会空间的逐步融合，攻击武器和攻击方式复杂多样，攻击组织经常会利用跨网跨域的手段实施渗透，躲避网络空间原有的安全防护措施。例如，通过社会工程猜测破解重要信息系统的账号与口令，利用地理定位信息实施物理层接入攻击，或者采用欺诈手段非法获取重要信息系统

① 国家互联网信息办公室. 国家网络空间安全战略. (2016-12-27). http://www.cac.gov.cn/2016-12/27/c_1120195926.htm.

② 王伟光. 牢牢掌握意识形态工作领导权管理权话语权. (2013-10-08). http://theory.people.com.cn/n/2013/1008/c40531-23117496-2.html.

的访问权限等。

针对电力、能源、交通、金融等关键基础设施的攻击活动一旦成功，将极大影响相关行业的正常运行。网络空间的攻击破坏可以迅速蔓延到物理空间和社会空间，影响经济运行，造成社会职能瘫痪，甚至破坏国家安全。其中，电力和能源系统是遭受网络攻击的“重灾区”。2015 年 12 月，乌克兰电网被黑客攻击瘫痪，造成大范围的供电中断。攻击者具备高度的组织化并且拥有丰富的资源支持，有数据表明超过 27 家变电站系统在这次攻击中被破坏[③]。2021 年 5 月，美国大型成品油管道系统运营商科洛尼尔管道运输公司因黑客通过非法软件控制其电脑系统，不得不临时关闭设备。科洛尼尔管道运输公司表示，这次网络袭击包含了勒索软件攻击。针对本次事件，美国气候政策实验室研究教授艾米·迈尔斯·贾菲表示：“这不仅是一条输油管道，而可以说是已经接近美国基础设施的大动脉了。”

由此可见，网络威胁早已突破了传统网络空间的时空限制，在威胁方式、攻击手法、影响范围和灾难性后果等方面，都已经扩展到了现实的物理空间和社会空间，成为跨领域、跨空间的综合性威胁因素。

1.3 精准打击与大范围破坏紧密结合

网络空间对抗各方在各自战略的统一指挥下，综合运用多种资源、多种战术、多种武器装备来实施对抗，既需要能够对大范围战术目标进行破坏的攻击工具（如能够感染对方大量设备造成系统瘫痪的蠕虫病毒），也需要能够重点突破战略目标的特殊手段（如针对对方核心设备的特种木马病毒）。残酷的网络空间对抗将时刻面临对方利用精准打击和大范围破坏紧密结合的实战场景。因此，维护网络空间安全需要有效应对不同类型的攻击手段和战术。

大范围破坏性攻击主要利用关键信息基础设施软硬件设备的同构性缺陷。计算机软硬件设备由于基于相同或相似的计算架构，安全漏洞具有极强的扩散和辐射效应。例如，Struts 2 作为阿帕奇（Apache）软件项目的全球广域网（web）框架，被众多商业网站开发者所使用。当 Struts 2 存在安全漏洞时，所有基于该框架开发的网站应用（包括知名的互联网站和电子商务平台）都面临严重的安全威胁。攻击者可以利用漏洞获得网站的控制权限，恶意篡改网站内容或植入后门程序。因此，网络攻击武器可以突破传统武器在地域和空间方面的限制，在极短时间内借助互联网络达到在同构设备间快速蔓延并造成大规模破坏的攻击效果。

精准打击则主要针对特定领域、特定装备、特定设施，利用零日漏洞、特种木马病毒等手段实施破坏，以期精准入侵并控制目标系统设施，达到直击对方要害，控制对方核心目标的效果。近年来，除了工控设备和物联网（IoT）设备以外，针对安全设备的攻击破坏也逐渐成为趋势。由于安全设备通常拥有较高的系统权限，一旦被突破将会造成灾难性后果。安全防护设备如果自身存在设计缺陷、安全漏洞或管理不善，不但起不到有效的保护作用，甚至会成为网络空间攻防对抗的关键薄弱点。目前，这一问题已经引起相关部门和重要行业的高度重视。

2 对策

当今世界，一场新的全方位综合国力竞争正在全球展开。能不能适应和引领互联网发展，成为决定大国兴衰的一个关键。世界各大国均把信息化作为国家战略重点和优先发展方向，围绕网络空间发展主导权、制网权的争夺日趋激烈，世界权力图谱因信息化而被重新绘制，互联网成为影响世界的重要力量。谁掌握了互联网，谁就把握住了时代主动权；谁轻视互

③ 4 E-ISAC. ICS Defense Use Case No.6: Modular ICS Malware. (2017-08-02). https://www.eisac.com/cartella/Asset/00006542/TLP_WHITE_E-ISAC_SANS_Ukraine_DUC_6_Modular_ICS_Malware_Final.pdf?parent=64412.

联网，谁就会被时代所抛弃。

为了做好网络空间安全保障工作，掌握网络空间的主动权和话语权，维护网络安全，迫切需要我们采取有效的应对策略和措施。

2.1 借鉴新冠肺炎疫情防控理念，织密网络空间保护网

2020年初以来，面对突如其来席卷全球的新冠肺炎疫情，我国充分发挥体制机制优势，采取了层层责任落实、严格管控高危人员、加强社区管理、保持社交距离、培养个人卫生习惯、推广疫苗接种等一系列有力措施，在取得良好防控成效的同时，保证了国民经济的稳步、健康发展。这次成功的抗疫行动，让我们看到了社会主义体制的优势，也为网络空间安全工作提供了新的启示。生物病毒是人类共同的敌人，网络威胁是网络空间共同的对手。网络威胁在威胁方式、破坏力、传播性、易感群体等方面呈现出诸多与生物病毒相似的特性。针对生物病毒的防控手段对网络空间的安全防范工作有着重要的借鉴意义。以典型的网络病毒为例，可以通过开展以下工作实现有效防控。

*（1）建立网络安全态势感知能力。*在第一时间准确、敏锐地感知尚处于初级传播阶段却具备巨大潜在威胁的网络病毒，实现网络病毒的早期预警，提早部署防范控制措施。

*（2）借鉴生物领域对人群的分类，划分网络主机类别。*围绕网络病毒的感染和传播问题，将网络主机划分为已感染主机（确诊病例）、疑似感染主机（疑似病例）、隐蔽感染主机（无症状感染者）、易感主机（密切接触者）、免疫主机（疫苗接种者）等类型。

*（3）针对不同类型的主机，分类采取措施。*分类采取断网（封闭治疗）、网络隔离（社区隔离）、补丁安装（接种疫苗）、系统加固（提高抵抗力）等手段，实现源头抑制和分类管控策略，将网络病毒的传播范围限制在尽可能小的区域内，有效阻断网络病毒的传播渠道。

如同疫情防控一样，在当今万物互联的时代，纯粹采取原有孤立的、封闭的安全保护措施，无法满足网络信息系统的互联互通需求。必须通过压实各级责任、落实制度要求、提升重点目标防范水平、监测感知重大网络威胁、提高应急响应效率、实施可信计算技术措施等一系列“组合拳”，多管齐下织密网络空间保护网，从而提高网络信息系统在面对网络威胁时的防范能力、应对能力和生存能力。

2.2 依托技术手段，打造关键信息基础设施安全堡垒

我国高度重视关键信息基础设施安全保护工作。关键信息基础设施是我国经济社会运行的神经中枢，是网络安全保护的重中之重，是构建国家网络空间安全保障体系的坚强堡垒。加强关键信息基础设施安全保护，对于维护国家安全、保障经济社会健康发展、维护人民群众根本利益意义重大。

针对国家关键信息基础设施面临的网络空间威胁，相关部门组织制定了《关键信息基础设施安全保护条例》，对涉及国计民生的关键信息基础设施保护范围作出规定，明确提出各方的安全职责和要求。关键信息基础设施保护是在落实网络安全等级保护制度的基础上，突出保护重点，强化保护措施，主要工作内容包括以下3点。

*（1）组织认定关键信息基础设施。*重点针对公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务、国防科技工业等重要行业和领域，掌握关键信息基础设施底数。

*（2）明确关键信息基础设施安全保护工作的职能分工。*包括公安部门、电信主管部门、关键信息基础设施安全保护工作部门和运营者，做到职责清晰。

*（3）落实关键信息基础设施重点防护措施。*针对关键信息基础设施的网络威胁有别于通用威胁。攻击

者可以利用零日漏洞，专项开发新型的恶意代码，绕过关键信息基础设施原有的网络安全防护措施并成功实施攻击。在这种情况下，依赖于攻击特征匹配的传统防护措施将会失效，必须依托以人工智能为代表的新型网络安全技术，通过对系统运行和网络应用服务的机器学习与分析建模，发现有别于正常访问的数据流量和操作行为，及时识别出重大网络威胁和攻击企图，从而不断提升关键信息基础设施的纵深防御和主动防御能力。

2.3 加强重点研发，支撑数据安全保护工作

数字经济为人民群众提供便利的同时，利用数据侵害人民群众合法权益的问题日益突出。《数据安全法》贯彻落实总体国家安全观，聚焦数据安全领域的风险隐患，是维护人民群众合法权益的客观需要，让人民群众在数字化发展中获得更多幸福感、安全感；该法的颁布实施也是促进数字经济健康发展的重要举措，通过促进数据依法合理有效利用，充分发挥数据的基础资源作用和创新引擎作用。《数据安全法》是国家大数据战略中至关重要的法制基础，也是数据安全保障和数字经济发展领域的重要基石。贯彻落实《数据安全法》，需要加强数据安全保护关键技术的研发工作，重点内容包括以下 4 个方面。

（1）*数据安全隐患主动探测技术*。基于漏洞挖掘和渗透测试技术方法，研究通过算法破译、协议漏洞、系统入侵、侧信道攻击等方式对数据安全隐患进行探查，主动发现数据采集、汇聚、存储、处理、分析、共享、使用等各个环节存在的安全隐患。

（2）*高强度算法与轻量级密码应用相结合的数据保护技术*。网络空间覆盖生产生活的方方面面，不同的应用领域在安全保护的强度、资源和便利性方面存在较大差异。因此，需要根据应用领域的实际需求，采取高强度和轻量级相结合的密码算法及应用配置。例如，针对大数据平台、云计算平台、工业控制系统、移动支付等高敏感数据的应用场景，采用高强度密码算法和安全协议保护数据存储及通信过程；而针对网络社交、媒体娱乐、普通商品交易等非敏感数据的应用场景，则通过使用轻量级密码算法，保证在受限的计算资源及存储资源条件下，提供足够强度的保护能力，在安全能力与资源投入方面取得更好的平衡。

（3）*支持隐私保护的数据安全分享技术*。数据分享是大数据时代永恒的话题。电子商务、协同办公、网络安全防护等各个领域均需要对海量数据进行分析挖掘。如何在实现高效分享的同时，保证数据源中包含的隐私内容不被泄漏和恶意利用，是当前数据安全领域亟待解决的技术问题。鉴于区块链技术具备去中心化和账户匿名性的特点，研究人员提出了基于区块链构建网络安全威胁数据共享模型，利用区块链的回溯能力实现对网络攻击链的追溯还原，从而为网络安全大数据应用环境下的隐私保护提供了新的技术思路。

（4）*面向数据交易的安全监管支撑技术*。作为新型的交易商品，数据交易的价值评估、支付方式和交付渠道与传统的实物类商品交易存在较大差异，需要针对其交易过程的各个环节开展网络安全监管，特别是数据类商品是否存在隐私泄露、非法交易、信息欺诈等违法行为。针对这一问题，需要针对交易方身份认证、内容合规性审查、可信溯源、交易标记、支付安全等关键技术进行攻关，促进数据的合法合规使用，实现数据交易与经济运行和社会流通的深度融合。

大数据时代，数据安全问题关系到国民经济发展和社会稳定，关系到国家安全。在现有法律法规的基础上，需要我们综合运用技术手段、管理制度、保障机制等方面的措施，维护数据全生命周期安全，实现国家网络空间安全保障体系的重点保护。

2.4 补齐产业短板，提升供应链安全保障水平

信息技术设备设施通常包含复杂的供应链关系。

以通用的计算存储服务器为例，机箱、电源、处理器、内存、硬盘、主板、显卡、光电模块、操作系统、数据库管理系统、应用软件等可能均由不同的原始厂商生产，各类设备设施组成的系统也是由多个技术服务厂商提供系统集成和后期运维管理。供应链中任何一个环节出现漏洞、缺陷或存在恶意设置的“后门”，都将会对设备设施乃至整个系统的安全带来致命影响。

近年来，围绕芯片制造、5G 通信、精密仪器、高端装备制造等高科技领域，西方发达国家对我国采取了一系列限制和打压政策。这再一次让我们清醒地认识到，加强供应链安全管理，以保证关键信息基础设施和网络信息系统的安全可信，是维护网络空间安全乃至国家安全的必要条件。因此，需要我们从以下 2 个维度开展工作。

（1）加快推进安全可信工程，扩展工程覆盖范围。从芯片、操作系统、数据库、网络安全产品，逐步扩展到板卡、主机、工业控制设备、嵌入式设备、便携设备、仪器仪表等信息技术各个细分领域，全面开展自主研发和安全可信升级替代，建立完善的、自主可控的信息技术领域供应链，以避免在关键环节受制于人。

（2）加强对信息技术产品和系统的供应链的管理。从产品和系统的设计、生产、调试、安装、部署、运维、技术服务等各个环节加强管控，力争从源头解决网络空间的安全隐患，有效防范和化解供应链带来的网络安全风险，补齐国家网络空间安全保障体系的防护短板。

3 总结

随着网络信息技术的迅猛发展和广泛应用，特别是我国国民经济和社会信息化建设进程的全面加快，网络已经成为实现国家稳定、经济繁荣和社会进步的关键基础设施。同时必须看到，境内外敌对势力针对我国网络空间的攻击破坏、恐怖活动和利用信息网络进行的反动宣传活动日益猖獗，严重危害我国国家安全，影响我国信息化建设的健康发展。网络安全是我们当前面临的新的综合性挑战。它不仅仅是网络本身的安全，而是关涉到国家安全和社会稳定，是国家安全在网络空间中的具体体现。当前，我国面临着复杂多变的国际形势，网络安全问题时刻影响着政治、经济、军事、文化、科技等各个领域[④]。

为了应对日益严峻的国际网络安全形势，有效防范敌对势力针对我国的网络攻击和渗透，必须掌握网络空间自主权和主导权。因此，需要从政策、法律、技术、制度、体制、机制、标准等各个方面多管齐下，织密网络空间保护网，落实关键信息基础设施保护制度，重点加强数据安全和供应链安全保障能力，建立起国家网络空间的安全屏障，为新时代中国特色社会主义建设和发展保驾护航。

参考文献

1 李艳. 美国强化网络空间主导权的新动向. 现代国际关系. 2020, 30(6): 73-90.

④ 谢永江. 人民网理论频道：习近平总书记的网络安全观. (2016-05-16). http://theory.people.com.cn/GB/n1/2016/0516/c386965-28354614.html.

Challenges to Cyberspace Security and Countermeasures

FENG Dengguo　LIAN Yifeng*

(Institute of Software, Chinese Academy of Sciences, Beijing 100190, China)

Abstract　The global cyberspace security situation continues to evolve, with the external environment becoming increasingly severe. Cybersecurity issues constantly affect politics, economy, military affairs, culture, scienceand technology, and other fields. In order to effectively prevent significant cyber threats and improve cyberspace autonomy and right of voice, we need to clearly understand the security challenges to cyberspace, implement the security protection of critical information infrastructure, and focus on strengthening the data security and supply chain security, so as to establish and improve the national cyberspace security system.

Keywords　cyberspace security, critical information infrastructure, data security, supply chain security



冯登国　中国科学院院士，中国科学院软件研究所研究员。长期从事网络与信息安全研究工作。曾任国家“863”计划信息安全技术主题专家组组长，国家“973”计划项目首席科学家，国家信息化专家咨询委员会委员等。发表论文200余篇，主持研制国际和国家标准20多项，荣获国家科技进步奖一等奖、国家技术发明奖二等奖等多项奖励。E-mail: fengdg@iscas.ac.cn

FENG Dengguo　Academician of Chinese Academy of Sciences (CAS), and researcher of Institute of Software, CAS. Dr. Feng has been engaged in network and information security research for a long time, published more than 200 papers, presided over the development of more than 20 international and national standards, and won many awards such as the first prize of National Science and Technology Progress Award and the second prize of National Technology Invention Award. He served as the leader of the expert group on information security technology of the National 863 Plan Project, the chief scientist of the National 973 Plan Project, and a member of the Advisory Committee for State Informatization Expert, etc. E-mail: fengdg@iscas.ac.cn



连一峰　中国科学院软件研究所研究员。中国网络安全审查技术与认证中心IT产品信息安全认证专业技术委员会副主任委员，信息安全等级保护关键技术国家工程实验室专家委员会委员，贵州省大数据及网络安全专家委员会委员。主持国家自然科学基金、国家重点研发计划等20余项重要科技项目。发表论文60余篇，出版专译著4部，发明专利17项，国家技术标准4项。E-mail: yifeng@iscas.ac.cn

LIAN Yifeng　Researcher of Institute of Software, Chinese Academy of Sciences (CAS), Vice Chairman of IT Product Information Security Certification Professional Technical Committee of China Cybersecurity Review Technology and Certification Center, Member of Expert Committee of National Engineering Laboratory for Key Technology of Classified Information Security Protection, and Member of Guizhou Data and Network Security Expert Committee. He presided more than 20 important scientific and technological projects, the sponsorships including National Natural Science Foundation of China and National Key Research and Development Program of China. In addition, he has published over 60 papers, 4 monographs, 17 patents and 4 national standards. E-mail: yifeng@iscas.ac.cn

■责任编辑：文彦杰

*Corresponding author